Department of Homeland Security Daily Open Source Infrastructure Report for 18 August 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a track fire in a New York City tunnel forced the evacuation of several thousand commuters in two subway trains at the height of the Wednesday, August 16, evening rush hour. (See item 17)
- The Associated Press reports West Virginia's Tri−State Airport was evacuated Thursday, August 17, after a bomb−sniffing dog reacted to a bottle filled with liquid in a passenger's luggage. (See item 19)
- The Los Angeles Times reports drug−resistant Staphylococcus aureus infections −− rarely seen in patients a decade ago −− have become the leading type of skin infections treated in emergency rooms. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 18, Associated Press* — **Disaster exercise covers three states.** Southeastern Alabama is the epicenter of an exercise this week testing officials' ability to respond to a major nuclear accident −− one almost on a scale of the nation's worst nuclear disaster in 1979 at the Three−Mile Island Nuclear Power plant in Pennsylvania. The National Nuclear Security

Administration kicked off the exercise with a scenario involving hundreds of federal, state and local officials: A truck carrying radioactive cesium, a common chemical with many medical and industrial uses, collided with a car at a rural southeastern Alabama intersection, triggering an explosion that unleashed a drifting plume of the potentially cancer−causing substance over towns, forests, and agricultural fields. In response, officials ordered mock evacuations, arranged emergency medical care for people who may have been severely contaminated and monitored the spread of the radioactive cloud. Federal monitoring teams will go out to test radioactive levels in soil, water, air, fish, and vegetation and report back to a command center, where scientists will analyze the information and make recommendations to state and local emergency officials.
Source: http://www.montgomeryadvertiser.com/apps/pbcs.dll/article?AID=/20060816/NEWS02/608160356/1009

2. *August 16, Associated Press* — **Security questioned in assault rifle delivery to nuclear plant.** The Project on Government Oversight (POGO) says a sealed crate containing 30 M−4 assault rifles delivered to a restricted area at the Tennessee Valley Authority's (TVA) Sequoyah Nuclear Power Plant created a security lapse, but TVA is not calling the June delivery of the rifles a security breach. TVA spokesperson John Moulton said the delivery was intended for TVA security personnel and contract security workers and arrived as planned. He said the rifles were inadvertently taken to another warehouse.
Source: http://www.wtvm.com/Global/story.asp?S=5290207&nav=menu91_2

3. *August 16, Bloomberg* — **OPEC lowers demand forecast as economic growth slows.** The Organization of the Petroleum Exporting Countries (OPEC) revised down its 2006 forecast for world crude demand as oil consumption fell unexpectedly among industrialized countries including the U.S. as global economic growth slowed. Growth in world oil demand will fall by 80,000 barrels a day to a daily average of 84.5 million barrels this year, from last month's forecast, OPEC said Wednesday, August 16, in its monthly report. Crude oil rose to record $74.80 in New York on July 14 on concern that fighting in Lebanon may spread in the Middle East, source of about a third of the world's oil. The International Energy Agency (IEA) left its forecast for 2006 world oil demand unchanged from a month ago at 84.8 million barrels a day, including biofuels, in its monthly report on August 11. Demand will reach 86.4 million barrels a day next year, an annual gain of 1.9 percent, the IEA said.
Source: http://www.bloomberg.com/apps/news?pid=20601100&sid=aZ5Bx0YT 3l0M

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *August 17, CBS 4 Boston* — **Leaking propane tank in New Hampshire prompts road and business closure.** A car hit a propane tank's meter Wednesday afternoon, August 16, in Salem, NH. Several businesses were closed down for the day, electricity was shut off and Route 28 was shut down. Firefighters were unable to cap the 6,000−gallon tank, so the decision was made to burn off the remaining propane. The controlled burn continued Thursday and parts of Route 28 remained closed.
Source: http://cbs4boston.com/local/local_story_229113948.html

5. *August 17, Arizona Republic* — **Fuel leak from collision forces evacuation in Arizona.** A fuel truck and pickup truck collided Thursday morning, August 17, in Surprise, AZ, forcing the evacuation of residents and businesses within a quarter−mile of the site. The collision occurred at Bell and Citrus roads, west of Loop 303, resulting in flames and a series of small explosions.
Source: http://www.azcentral.com/news/articles/0817propaneleak17−ON− CR.html

[Return to top]

Defense Industrial Base Sector

6. *August 16, Network World* — **Military researching intelligent, secure wireless network.** The U.S. government, corporate and academic researchers are working on a network that would be able to configure itself, intelligently cache and route data, and allow for fast and reliable sharing of data, all while maintaining military−grade security. The project is called Knowledge Based Networking and is under development by the U.S. Department of Defense Research Projects Agency (DARPA). Academic concepts such as artificial intelligence and Tim Berners−Lee's "Semantic Web," combined with technologies such as the Mobile Ad−hoc Network (MANET), cognitive radio, and peer−to−peer networking, would provide the nuts and bolts of such a network. Preston Marshall, the program manager of DARPA's Advanced Technology Office, says that current technology is "dominated by wireless access, not really wireless networking." Instead of using access points to connect wireless devices to a wired network, a Knowledge Based Network would be a decentralized MANET. MANETs would be able to route traffic through an ever−changing set of peers to a networked device or the Internet. Such networks would have no single point of failure. More experimentation needs to be done before MANET technology can be standardized and mass−produced, but the Knowledge Based Networking initiative might provide incentive for military contractors to work on the technology.
Source: http://www.networkworld.com/news/2006/081606−intelligent−net work.html

[Return to top]

Banking and Finance Sector

7. *August 17, IDG News Service* — **Internet crimes hit record high in Japan.** The number of Internet−related crimes in Japan in the first six months of this year hit a record high, according to data issued Thursday, August 17, by the National Police Agency. Crimes involving illegal access to computer networks jumped 34 percent to 265 cases in the six−month period. These included cases where people accessed accounts on online gaming services, access to Internet banking accounts, and phishing attacks, where people are tricked into revealing their user names and passwords.
Source: http://www.infoworld.com/article/06/08/17/HNinternetcrimesja pan_1.html

8. *August 17, Honolulu Advertiser* — **Latest phishing scam targets Kauai.** The Kauai Community Federal Credit Union on Wednesday, August 16, became the latest Hawaii financial institution to be targeted by phishing scams that have ensnared six local financial institutions to date. The Kauai credit union joined Hawaii State Federal Credit Union, Hawaiian Tel Federal Credit Union, Bank of Hawaii, First Hawaiian Bank, and American Savings Bank

as a target of a phishing scam within the past year. The e−mails look official, with logos of the institutions and requests to change passwords or confirm or update information. The Kauai credit union placed a warning on its Website.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060817/NEWS01/608170344/1001

9. *August 16, Websense* — **Phishing Alert: Bank of Austria Creditanstalt.** Websense Security Labs has received reports of a new phishing attack that targets customers of Bank of Austria Creditanstalt. Users receive a spoofed e−mail message claiming that many fraudulent transactions have been discovered, and that users must follow new security procedures. The URL provided by the e−mail is a phishing site that attempts to collect users' account information such as transaction authentication number (TAN) and personal identification number (PIN).
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=577

10. *August 16, Websense* — **Phishing Alert: Banco Regional de Monterrey (eBanRegio).** Websense Security Labs has received reports of a new phishing attack that targets customers of Banco Regional de Monterrey. Users receive a spoofed e−mail message claiming that their account has been accessed from multiple IP addresses and this activity must be verified. The URL provided in the e−mail is a phishing site that attempts to collect users' account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=578

11. *August 16, Websense* — **Phishing Alert: Tribunal Superior Eleitoral.** Websense Security Labs has received reports of a new phishing attack that targets customers of the Brasilian Tribunal Superior Eleitoral. Users receive a spoofed e−mail message claiming that their entry in the electoral roll has been cancelled. To learn the reason for the cancellation and be able to reinstate their right to vote at the upcoming elections, users must read the attached regulations. The link provided by the e−mail leads to a download for a Trojan that installs malicious code on the user's computer.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =576

12. *August 16, IDG News Service* — **Yahoo plugs security hole in Web mail service.** Yahoo Inc. has fixed a security vulnerability in its Yahoo!Mail service that could have allowed malicious hackers to hijack accounts and harm users in a variety of ways. "We have developed a fix for this bug and have deployed it worldwide. Yahoo!Mail users will not be required to take any action to be protected from this exploit," said Kelley Podboy, a Yahoo spokesperson.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002506&taxonomy Id=17

13. *August 16, Computer World* — **Survey: 81 percent of U.S. firms lost laptops with sensitive data in the past year.** Loss of confidential data −− including intellectual property, business documents, customer data and employee records −− is a pervasive problem among U.S. companies, according to a survey released Tuesday, August 15 by Ponemon Institute. Eighty−one percent of companies surveyed reported the loss of one or more laptops containing sensitive information during the past 12 months. One of the main reasons corporate data security breaches occur is because companies don't know where their sensitive or confidential

business information resides within the network or enterprise systems, said Larry Ponemon of the Ponemon Institute. "This lack of knowledge, coupled with insufficient controls over data stores, can pose a serious threat for both business and governmental organizations," Ponemon said. "Moreover, the danger doesn't stop at the network, but includes employees' and contractors' laptop computers and other portable storage devices."
Survey: http://www.vontu.com/uploadedFiles/global/Ponemon−Vontu_US_Survey−Data_at−Risk.pdf
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002493&taxonomy Id=17

[Return to top]

Transportation and Border Security Sector

14. *August 17, RAND Corporation* — **Report: Considering the effects of a catastrophic terrorist attack on the Port of Long Beach.** In recent years, there has been a growing concern that targeted acts of terrorism, focused on critical economic infrastructure, could produce cascading social and economic effects on a very wide scale. In this report, two RAND Corporation technical authors carry out a scenario analysis and strategic gaming revolving around a catastrophic terrorist attack on the Port of Long Beach. The authors describe the results from this investigation and provide many of the primary results from the analysis in the appendixes. The analysis tools developed by the authors for this study lay the groundwork for research exploring both the short− and long−term effects of catastrophic events. The need is pressing to continue such investigations, particularly of longer−term economic repercussions. The overarching goals would be to gain insight into the decision landscape in the months following attacks of this magnitude with a focus on identifying where existing systems are likely to fail and evaluating the benefits of a range of potential economic policies. With these types of tools, policymakers could start to anticipate the types of decisions they might be called upon to make, reflect in times of relative calm on their options, and plan in advance for contingencies.
Report: http://www.rand.org/pubs/technical_reports/2006/RAND_TR391.p df
Source: http://www.rand.org/pubs/technical_reports/TR391/

15. *August 17, AdelaideNow (Australia)* — **Plane surrounded at Sydney Airport.** Passengers on an international flight were evacuated from a plane at Sydney Airport in Sydney, Australia, on Thursday, August 17, after a threat was made against the aircraft. "A Pacific Blue flight from Nadi, Fiji, which landed at approximately 5.45 p.m. (AEST) today has had a threat made against it," Sydney Airport Corporation spokesperson Peter Vickary said. The Seven Network says the threat against the 737 aircraft was made from the Philippines .. while the plane was en route from Fiji. Police said authorities are investigating reports of a suspicious device on board the plane. "Emergency services and airport authorities are currently examining an aircraft at Sydney Airport following unconfirmed reports that a suspicious device may be on board," a police spokesperson said.
Source: http://www.news.com.au/adelaidenow/story/0,22606,20162677−50 05962,00.html

16. *August 17, Associated Press* — **NWA attendants can walk out August 25.** A federal bankruptcy judge on Thursday, August 17, denied a Northwest Airlines Corp. (NWA) request to block a strike by its flight attendants that could begin as soon as August 25. Judge Allan

Gropper in New York wrote that he does not have the authority to block a strike as Northwest had requested. Flight attendants have said they may begin random, unannounced strikes after 10:01 p.m. EDT August 25 unless Northwest negotiates a new contract with them. Northwest imposed pay cuts and work rules on flight attendants last month after they voted down a negotiated settlement. The union has not said what kind of strike it plans; it could range from a occasional, unannounced strikes at specific gates or flights to a full−scale walkout. The idea is that even small−scale disruptions can cause passengers to book away from an airline, giving the union leverage.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20060817/NEW S99/60817017

17. *August 17, Associated Press* — **Fire prompts thousands to evacuate subway trains.** Service was restored after a track fire in a New York City tunnel forced the evacuation of several thousand commuters in two subway trains at the height of the Wednesday evening rush hour on August 16. At least 25 people received minor injuries in the incident. More than a dozen people, including three firefighters, were treated at hospitals for smoke inhalation, officials said. Between 3,000 and 4,000 people were evacuated from the B− and D−line subway trains, the fire department said. The fire halted the two 10−car trains on the lower level of the Manhattan Bridge, which spans the East River between Manhattan and Brooklyn. Three cars on one of the Brooklyn−bound trains were inside the tunnel, which leads to the borough's DeKalb Avenue subway station, while the other train was stopped behind the first. More than 100 firefighters and rescue workers responded to the fire, which was reported by a train operator around 6 p.m. The blaze was declared under control about 8 p.m. Assistant Fire Chief James Esposito said, investigators found trash and cigarette butts around where the fire started, near what appeared to be a homeless encampment. The cause of the blaze was being investigated, Esposito said.
Source: http://www.wnbc.com/traffic/9691551/detail.html

18. *August 17, Department of Transportation* — **FRA to revise rail safety rules to support deployment of improved train braking technology.** Calling it the most significant development in railroad brake technology since the 1870s, Federal Railroad Administrator (FRA) Joseph H. Boardman announced on Thursday, August 17, his intention to propose revised federal rail safety regulations to facilitate the installation of Electronically Controlled Pneumatic (ECP) brake systems capable of preventing derailments and shortening train−stopping distances. “ECP brakes are to trains what anti−lock brakes are to automobiles −− they provide better control,” Boardman said. Boardman said the FRA intends to issue a notice of proposed rulemaking next year to revise the federal brake system safety standards to encourage railroads to invest in and deploy ECP brake technology. In order to achieve the safety benefits as soon as possible, FRA is open to considering plans from railroads interested in using ECP brakes before the proposed rule changes are completed, he said. In 2005, 14 percent of train accidents on main line track caused by human error involved improper train handling or misuse of the automatic braking system. ECP brakes would give locomotive engineers better control over their trains and prevent many potential accidents.
Source: http://www.dot.gov/affairs/fra1006.htm

19. *August 17, Associated Press* — **West Virginia airport terminal evacuated.** A West Virginia airport terminal was evacuated Thursday, August 17, after a bomb−sniffing dog reacted to a bottle filled with a liquid in a passenger's luggage, an airport official said. The Tri−State

Airport was evacuated and flights canceled Thursday because security officials feared a passenger's water bottle might contain a liquid explosive. A Transportation Security Administration (TSA) official said the water bottle first screened positive for what could be an explosive material at 9:15 a.m. EDT. That test was then confirmed at 11:25 a.m. by a TSA explosive detection canine team. The airport, near West Virginia's border with Kentucky and Ohio, was then evacuated. "It's an inconvenience, but we are pleased that it was found when it was, rather than on the plane," said Jim Booten, president of the Tri−State Airport Authority. US Airways spokesperson Andrea Rader confirmed that the passenger with the bottle was a woman who was scheduled to leave Huntington on U.S. Airways 4168 to Charlotte, NC, at 9:17 a.m. The flight left without the passenger or her baggage.
Source: http://www.usatoday.com/news/nation/2006−08−17−terminal−evac uated_x.htm

20. *August 16, New York Times* — **Faces, too, are searched at U.S. airports.** Taking a page from Israeli airport security, the Transportation Security Administration has been experimenting with a new squad, whose members do not look for bombs, guns or knives. Instead, the assignment is to find anyone with evil intent. So far, these specially trained officers are working in only about a dozen airports nationwide, including Dulles International Airport outside Washington, DC, and they represent just a tiny percentage of the transportation agency's 43,000 screeners. But after the reported liquid bomb plot in Britain, agency officials say they want to have hundreds of behavior detection officers trained by the end of next year and deployed at most of the nation's biggest airports. Concerns, however, have been raised by two of the foremost proponents of the techniques, a former Israeli security official and a behavioral psychologist who developed the system of observing involuntarily muscular reactions to gauge a person's state of mind. They said in interviews that the agency's approach puts too little emphasis on the follow−up interview and relies on a behavior−scoring system that is not necessarily applicable to airports.
Source: http://www.nytimes.com/2006/08/17/washington/17screeners.htm l?hp&ex=1155873600&en=0d7d13a17ac78eb2&ei=5094&partner=homep age

21. *August 15, Department of Homeland Security* — **US VISIT deploys biometric entry procedures to additional locations.** The Department of Homeland Security (DHS) has announced the expansion of the US VISIT program's biometric entry procedures to additional locations in Fresno, CA, New Orleans, LA, and Halifax, Canada. US VISIT's biometric entry procedures – digital, inkless finger scans and digital photograph – are a part of the routine primary inspection process at airports and seaports with international arrivals, in the secondary inspection areas of U.S. land border ports of entry and at U.S. consulates around the world – through the State Department's complementary program called BioVisa. No changes will be made to the US−VISIT process or to the classifications of travelers subject to US−VISIT as the result of this expansion. US VISIT currently applies to most visitors (with limited exemptions) entering the United States, regardless of country of origin or whether they are traveling with or without a visa or by air, sea or land. US−VISIT does not apply to most Canadian travelers. Since the program launched in 2004, more than 62 million people have been processed through US VISIT at U.S. ports of entry. With the help of US−VISIT biometric procedures, more than 1,200 criminals or immigration violators have been denied entry to the United States.
For more information, visit the US VISIT Website at http://www.dhs.gov/us−visit
Source: http://www.dhs.gov/dhspublic/display?content=5804

[Return to top]

Postal and Shipping Sector

22. *August 16, Union−Tribune (CA)* — **Mail stolen from three postal trucks in San Diego.** Three U.S. Postal Service trucks have been broken into since mid−July in southeastern San Diego, and several pieces of mail have been stolen, authorities announced on Tuesday, August 15. Thieves smashed the passenger−side windows of the trucks, which all were parked and locked at the time, said U.S. Postal Inspector Hilary A. Smith. The thefts occurred during regular business hours as the carriers delivered mail, Smith said. All customers who might have been affected have been notified by mail, Smith said. One flat of mail was taken from each truck but no parcels or packages were taken, Smith said. While the motives for the thefts are unknown, they may have been for identity theft −− to use the documents for fraud. Smith warned postal customers to be vigilant when checking their mail. She urged them to watch for strange charges on credit card bills or accounts opened in different names.
Source: http://www.signonsandiego.com/news/metro/20060816−9999−7m16p ostal.html

[Return to top]

Agriculture Sector

23. *August 16, KTIV (IA)* — **Anthrax outbreak in South Dakota.** There's an outbreak of anthrax in southeast South Dakota, and the state veterinarian is urging livestock owners to take steps to protect their herds. Cattle died in South Dakota after they ingested naturally−occurring anthrax spores while they were grazing. State veterinarian Sam Holland believes runoff from recent rainfall may have exposed the spores. The outbreak of anthrax that killed three cows has been confirmed in a herd of about 50 cattle near of Lennox, SD.
Source: http://www.ktiv.com/News/index.php?ID=3408

24. *August 16, Stop Soybean Rust News* — **Soybean rust found in two more Louisiana counties.** Asian soybean rust was confirmed in two additional parishes, Avoyelles and Tensas in Louisiana. This brings the total to six Louisiana parishes in which soybean rust has been found on either soybeans or kudzu. These finds are the first reports of rust for these counties. Currently rust has been found on this year's soybeans in twelve different counties in five states (Alabama, Florida, Georgia, Louisiana and Mississippi), the rest of the finds have been on kudzu. A total of 32 counties have reported rust this year and include five in Alabama, 13 in Florida, six in Georgia, six in Louisiana, one in Texas, and one in Mississippi.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=917

25. *August 16, Stop Soybean Rust News* — **Rust found on sentinel plot in Baldwin County, Alabama.** On August 10, soybean rust was detected in a late−planted soybean sentinel plot in Baldwin County near the town of Fairhope, AL. The disease had been detected in an earlier planted soybean sentinel plot at the same location on June 27. That plot was destroyed shortly after discovery of the disease.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=918

[Return to top]

Food Sector

26. *August 16, Animal and Plant Health Inspection Service* — **Potato imports from Canadian province restricted.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Wednesday, August 16, announced that it is prohibiting the entry of potatoes and other products from the province of Quebec due to the detection of the golden nematode (GN), a serious pest of potatoes. "In the coming weeks, we will work closely with the Canadian Food Inspection Agency to analyze survey data and other information and will further regionalize our restrictions, if appropriate, based on the latest scientific evidence and in accordance with international guidelines," said APHIS Administrator Ron DeHaven. The Canadian Food Inspection Agency Tuesday, August 15, confirmed the presence of the pest in a 30−acre field on a farm east of Montreal, Quebec. GN can significantly affect the yields of potatoes and other host crops. To prevent the spread of the nematode to the U.S., officials are prohibiting potatoes for seed, consumption and processing from the Province of Quebec and requiring that other restricted articles from Quebec be free from soil.
Source: http://www.aphis.usda.gov/newsroom/content/2006/08/gn_Canadi an.shtml

27. *August 15, U.S. Food and Drug Administration* — **Salad, spreads, dips, and related products recalled.** Future Food Ltd, of Dallas, TX, is expanding its August 11, 2006 recall of Krab Dip Supreme and Supreme Krab Dip to include the following additional products; Krab Log, Cajun Smoked Salmon Flavored Spread, Krab Artichoke Spinach Dip, Krab Dip, Cajun Krab Dip, Jalapeno Krab Dip, Cajun Crawfish Salad, and Smoked Salmon Flavored Spread. These products were sold under the brand names of Salads of the Sea, Hen House, Southern Home and Fisherman's Market. The recall is being expanded because these products have the potential to be contaminated with Listeria Monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. The potential for contamination was noted after routine testing revealed that a package of Krab Dip Supreme, which was recalled on August 11, 2006, contained Listeria Monocytogenes. Because all of the products in this expanded recall were produced by the same manufacturer, on the same day and on the same equipment as the products recalled on August 11, Future Food is expanding the recall. The products were distributed in FL, SC, AL, KS, NC, VA, TN, OK, FL, MI, MO, AZ, NM, OH, WA, OR, CO, CA, and LA.
Source: http://www.fda.gov/oc/po/firmrecalls/future208_06.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

28. *August 17, Los Angeles Times* — **Hospitals report increase in drug−resistant staph infections.** Drug−resistant staph infections −− rarely seen in patients a decade ago −− have become the leading type of skin infections treated in emergency rooms, scientists reported Wednesday, August 16. The study in the New England Journal of Medicine was the first to demonstrate the extent to which drug−resistant Staphylococcus aureus has spread throughout the U.S. The bacterium accounted for 59 percent of skin infections in the study, researchers said, with ranges of 15 percent in New York City to 74 percent in Kansas City, MO. What triggered the spread of drug−resistant staph isn't known. Some years ago, researchers started finding infections in jail inmates, sexually active gay men, and professional athletes. Last year, infections were reported among the general population in Atlanta, Baltimore, and Minnesota. The study looked at 422 patients treated for skin and soft−tissue infections during August 2004. The patients were seen in university−affiliated emergency rooms in 11 cities. The staph was resistant to antibiotics routinely used to treat skin and soft−tissue infections, such as erythromycin; cephalexin, and dicloxacillin, scientists said.
Abstract: http://content.nejm.org/cgi/content/short/355/7/666
Source: http://www.latimes.com/news/nationworld/nation/la−sci−staph17aug17,1,684407.story?coll=la−headlines−nation

29. *August 17, Agence France−Presse* — **Indonesia probes possible cluster after 45th bird flu death.** Health authorities in Indonesia have begun investigating whether a nine−year−old girl who died of the H5N1 strain of bird flu belonged to a cluster of human cases. Cluster cases heighten the chance of the virus mutating to become easily transmissible between humans. Ai Siti Aminah was confirmed on Thursday, August 16, to have died of the H5N1 virus, which has now killed 45 Indonesians, the highest of any nation in the world. The victim came from Cikelet, a remote area in West Java's Garut district, and lived not far from the home village of 17−year−old Umar Aup, who tested positive for the virus and remains alive. The boy's 20−year−old cousin Misbah however died earlier this month while exhibiting signs of the virus.
Source: http://news.yahoo.com/s/afp/20060817/wl_asia_afp/healthfluin donesia_060817102031

30. *August 17, Food and Agriculture Organization* — **Both endemic and new virus strains to blame for bird flu recurrence in Asia's poultry.** Laboratory confirmation points to both old and new isolates of the bird flu virus as sources of recent highly pathogenic avian influenza (HPAI) outbreaks in Southeast Asia, the Food and Agriculture Organization (FAO) said Thursday, August 17. Concerned about the recurrence of bird flu in Asia, close monitoring of diagnostic results by FAO has revealed that bird flu is endemic in some areas while new strains have emerged in other places. "Last month's HPAI outbreak in Thailand's Pichit province was caused by the same virus strain circulating in the area since 2003/4. The H5N1 virus thus remained alive in central Thailand in a reservoir of birds and poultry, most probably a mix of backyard chicken, ducks and fighting cocks," said Laurence Gleeson, regional manager of FAO's bird flu center in Bangkok. This indicates that the H5N1 virus is endemic in the area. While the number and size of outbreaks has been reduced, past control efforts were only partly successful. On the other hand, the outbreaks in Nakhon Phanom and Vientiane were caused by a H5N1 virus strain previously not detected in Thailand and Laos. The virus is similar to recent isolates from southern China, suggesting that the virus spread from China.
Source: http://www.fao.org/newsroom/en/news/2006/1000377/index.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *August 17, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: An area of low pressure located approximately 120 miles east of Charleston, SC, has changed little over the past several hours while drifting westward. While there is still some potential for this system to become a tropical depression over the next 12 to 24 hours, upper−level winds are becoming increasingly unfavorable for development. Eastern Pacific: Tropical Storm 09E (Hector) is 1140 miles south of San Diego, CA. Hector is moving toward the west−northwest at 10 mph. Based on the current warning this system poses no threat to the U.S. Western Pacific: Tropical Storm 11W (Wukong) poses no threat to U.S. territories. Tropical Depression 12W (Sonamu) has dissipated. Earthquake Activity: A magnitude 4.5 earthquake occurred on Thursday, August 17, at 01:14 EDT in the Near Islands, part of the Aleutian Island chain in Alaska. The epicenter was 1460 miles west of Anchorage at a depth of 20.6 miles. No tsunami was generated.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat081706.shtm

32. *August 17, Washington Post* — **Group urges disaster planning for pregnant women, babies.** In the days after Hurricane Katrina struck Louisiana, about 125 critically ill newborn babies and 154 pregnant women were evacuated to Woman's Hospital in Baton Rouge. Katrina focused unprecedented attention on pregnant women and newborns as an acutely vulnerable population during emergencies. A year later, those concerns are driving a push to add provisions for both groups to national preparedness guidelines for disasters, epidemics or terrorist attacks. "Pregnant women face greater risks −− like premature births, low birth−weight babies and infant deaths −− during the stressful conditions of a disaster. This can make delivering a child difficult and potentially life−threatening," said Theresa Shaver, executive director of the District−based White Ribbon Alliance for Safe Motherhood. "International relief agencies have detailed guidelines for helping pregnant women, infants and new mothers in disasters around the world," she said. "But in the United States, it is not yet integral to our preparedness plans." The alliance has set up a working group to develop domestic guidelines in association with groups of pediatricians, gynecologists, obstetricians, nurses and midwives.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/16/AR2006081601516.html

33. *August 16, Federal Emergency Management Agency* — **Floodsmart.gov Website: A valuable resource.** The Federal Emergency Management Agency's (FEMA) FloodSmart Website is the official Website of the National Flood Insurance Program, which is administered by FEMA. The site has myriad resources home and business owners. On the site users can: a) enter an address into a form and find out how likely it is to flood; b) find local flood insurance agents; c)

estimate the cost of different depths of flood; and d) estimate flood insurance premiums. In addition, FEMA answers flood−related questions on its Website.
FloodSmart Website: http://www.floodsmart.gov/floodsmart/pages/index.jsp
Source: http://www.fema.gov/news/newsrelease.fema?id=28918

34. *August 16, Midwest City Sun (OK)* — **Oklahoma emergency management officials gather for conference.** Nearly 300 emergency managers and other local government officials gathered Wednesday and Thursday, August 17, at Midwest City, OK's, Reed Center for the Emergency Management Fall Conference. From all across the state the officials met for extensive discussions on the role of homeland security and emergency management in preparedness, response, recovery and mitigation efforts related to keeping our communities, state and nation safe. The conference was sponsored by the Oklahoma Department of Emergency Management and the Oklahoma Emergency Management Association.
Source: http://www.mwcsun.com/local/local_story_228120640.html

[Return to top]

Information Technology and Telecommunications Sector

35. *August 17, Security Focus* — **Symantec NetBackup PureDisk authentication bypass vulnerability.** Symantec NetBackup PureDisk is prone to an authentication bypass vulnerability. Analysis: Attackers may exploit this issue to gain administrative access to the vulnerable application. This may allow an attacker to gain administrative privileges on the underlying operating system.
Vulnerable: Symantec Veritas NetBackup PureDisk Remote Office Edition 6.0.
Solution: Symantec has released an update to address this issue. For more information: http://www.securityfocus.com/bid/19524/references
Source: http://www.securityfocus.com/bid/19524/discuss

36. *August 17, BBC* — **Speedy silicon sets world record.** A simple tweak to the way common silicon transistors are made could allow faster, cheaper mobile phones and digital cameras, say UK researchers. To achieve the speed gain, researchers at the University of Southampton added fluorine to the silicon devices. "It just takes a standard technology and adds one extra step," said Professor Peter Ashburn at the University of Southampton, who carried out the work. When the researchers tested the new device it clocked a speed of 110 GHz. Complete circuits usually operate at about a tenth of the speed of the component transistors. Although a product has not been built using the devices, Ashburn says they could be used to amplify the signal in mobile phones or to improve the way that handsets convert speech into digital signals. Complete circuits could also be used in digital cameras or scanners to improve the way they convert information from the real world into pixels.
Source: http://news.bbc.co.uk/1/hi/technology/5259594.stm

37. *August 17, CNET News* — **Security researchers want increased communication from software makers.** In recent years, software companies have hammered out rules with researchers on disclosure, which cover how and when vulnerabilities are made public. Now flaw finders want something in return: more information from software providers on what they

are doing to tackle the holes the researchers have reported. "Researchers want the vendors to be more aggressive, and the vendors want the researchers to show more discretion," said Gartner analyst Paul Proctor. Software vendors need to establish protocols for interacting with researchers who share bug information, experts said. If they don't, they could risk losing the progress that has been made towards responsible disclosure of flaws.
Source: http://news.com.com/Flaw+finders+to+software+makers+Its+payback+time/2100−1002_3−6106593.html?tag=nefd.lede

38. *August 17, Register (United Kingdom)* — **Holy Moly Website hacked; users redirected to malicious Website.** Celebrity gossip Website Holy Moly was hacked on Wednesday, August 16. The defacement of the site included re−direction script that attempted to load malware onto the PCs of surfers by sending them to a maliciously−constructed Website. Credit for the attack, whose precise motives remain unclear, was claimed by a Turkish person going by the handle "Iskorpitx," an active defacer whose previous targets have included Microsoft and hosting firm GoDaddy.
Source: http://www.theregister.co.uk/2006/08/17/holy_moly_hacked/

39. *August 17, Los Angeles Times* — **Attorney General: Extremists are homing in on the Internet.** Attorney Gen. Alberto R. Gonzales said Wednesday, August 16, that more than 5,000 Internet sites were being used by extremists to train and coordinate internationally, filling the gap caused by the crackdown on the Al Qaeda terrorist network. Gonzales' estimate suggests a significant expansion of the Internet infrastructure used by Islamic extremists in recent years to mobilize their efforts. Since late 2001, the United States and its allies have demolished Al Qaeda's home base in Afghanistan, killed or captured some of its leaders, cut off many outside funding channels and disrupted some means of communication. But those efforts have driven Al Qaeda members to the Internet, "where their ideology has inspired and radicalized others," Gonzales said in a speech to the World Affairs Council of Pittsburgh. "This radicalization is happening online and can therefore develop anywhere, in virtually any neighborhood, and in any country," said Gonzales.
Source: http://www.latimes.com/news/nationworld/nation/la−na−terror17aug17,1,2257285.story?coll=la−headlines−nation&track=crossp romo

40. *August 16, TechWorld* — **Consumer group condemned for creating 5,500 "test" viruses.** A consumer magazine has been condemned for possibly adding to the virus problem by creating a series of "test" viruses just to review anti−virus scanners. In an act that has long been considered technical taboo, U.S.−based consumer affairs organization, ConsumerReports.org, decided to generate 5,500 "test" viruses to run, under lab conditions, against 12 leading anti−virus software products. The organization’s own Website describes the methodology used: "To pit the software against novel threats not identified on signature lists, we created 5,500 new virus variants derived from six categories of known viruses, the kind you’d most likely encounter in real life." The organization said it had enlisted the help of Independent Security Evaluators, an external consultancy, to help design the tests and ensure they matched real−world conditions. While the viruses are not expected to pose any threat to companies or individuals, their creation of viruses is still controversial.
Source: http://www.techworld.com/security/news/index.cfm?newsID=6658 &pagtype=all

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 25 (smtp), 445 (microsoft−ds), 32790 (−−−), 113 (auth), 80 (www), 6346 (gnutella−svc), 5900 (vnc), 1433 (ms−sql−s) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

41. *August 16, Inside Bay Area (CA)* — **Baseball fans unknowingly pass scientists' sniff test.** As fans walked into McAfee Coliseum to see the Oakland A's play the Detroit Tigers and the Los Angeles Angels, scientists working for the Department of Homeland Security (DHS) were sniffing them −− their popcorn, their cigars, hairspray, and after−shave. The scientists, sent from Sandia National Laboratories, wondered whether they could catch a whiff of a terrorist chemical attack in this morass of smells. "We were very pleased with the background at the coliseum," said Ben Wu, project manager for Sandia's "rapidly deployable chemical detection system." DHS officials were keen to learn about open−air venues, especially those used for national security "special events" such as the Super Bowl and the Olympics. In a few years, they want to hone the system into a network of chemical sensors that require no more attention than a home smoke detector but could sniff an industrial toxin or nerve gas in time to evacuate thousands of spectators.
Source: http://www.insidebayarea.com/ci_4188974?source=rss

[Return to top]

General Sector

42. *August 17, New York Times* — **U.S. officials arrest suspect in top Mexican drug gang.** Federal drug enforcement agents, aided by the United States Coast Guard, arrested a man they said was a top figure in one of Mexico’s most notorious drug gangs on a fishing boat off Baja California on Wednesday, August 16. Federal officials said the man, Francisco Javier Arellano Félix, 37, was one of the last remaining ring leaders of the Arellano Félix gang. The group, based in Tijuana, is charged in several killings, including that of a Roman Catholic cardinal
Source: http://www.nytimes.com/2006/08/17/us/17drug.html?_r=1&oref=s login

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer